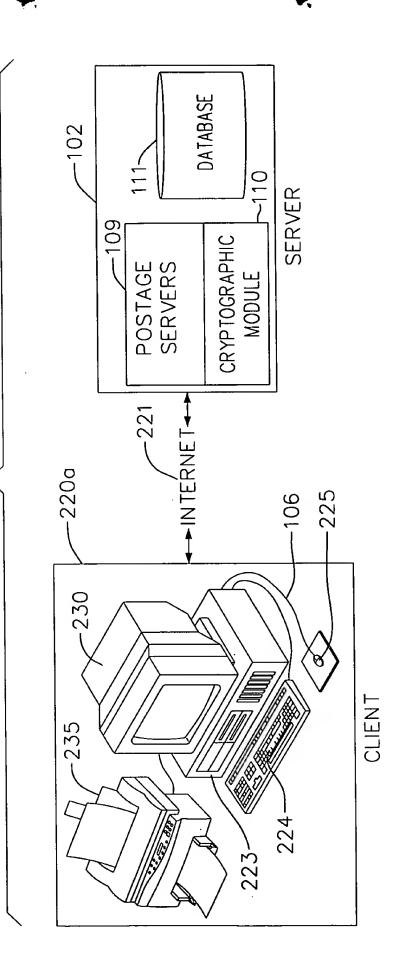
FIG. 1



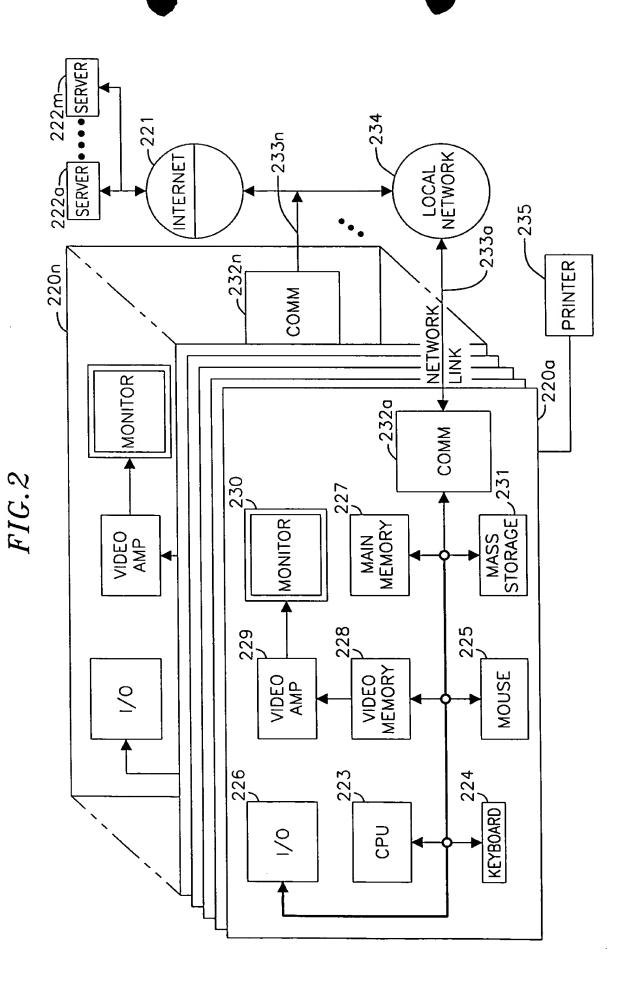
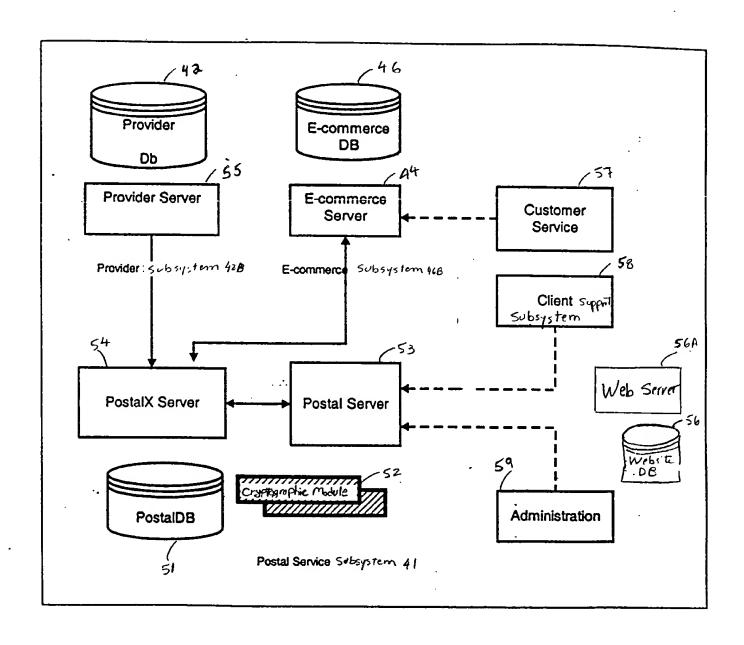
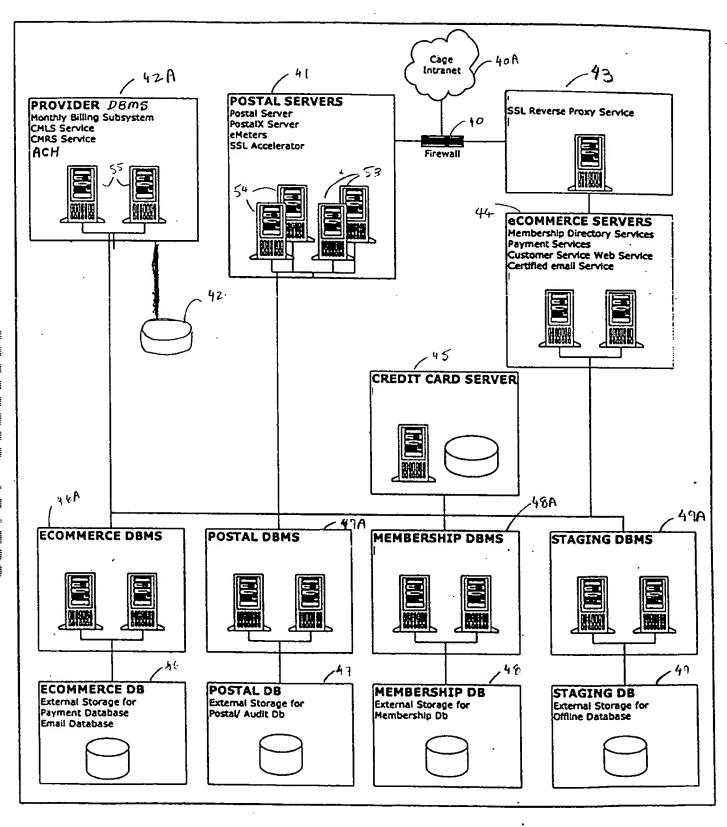
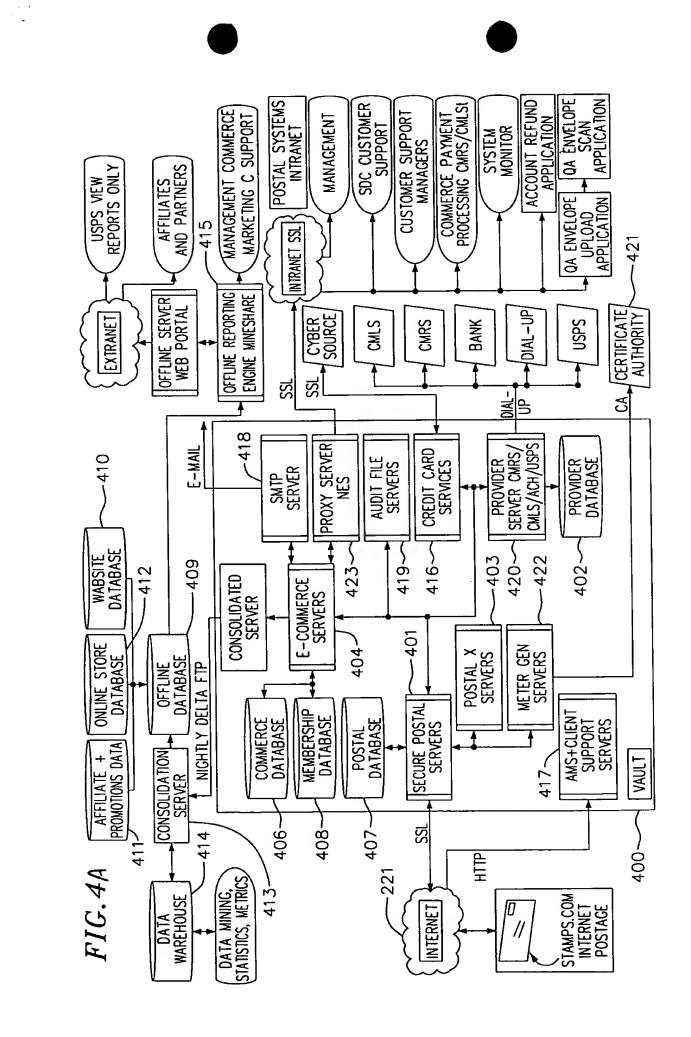


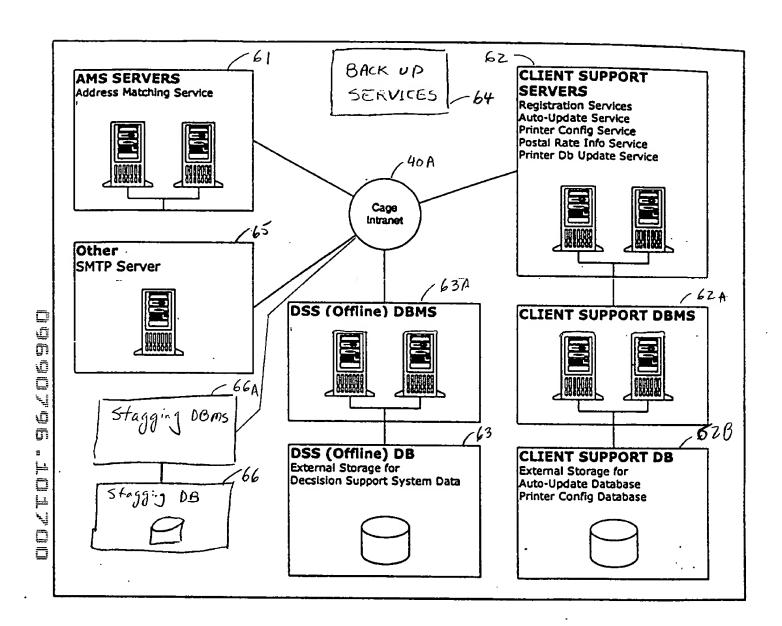
FIG. 3





OARDE" DOADGEGO





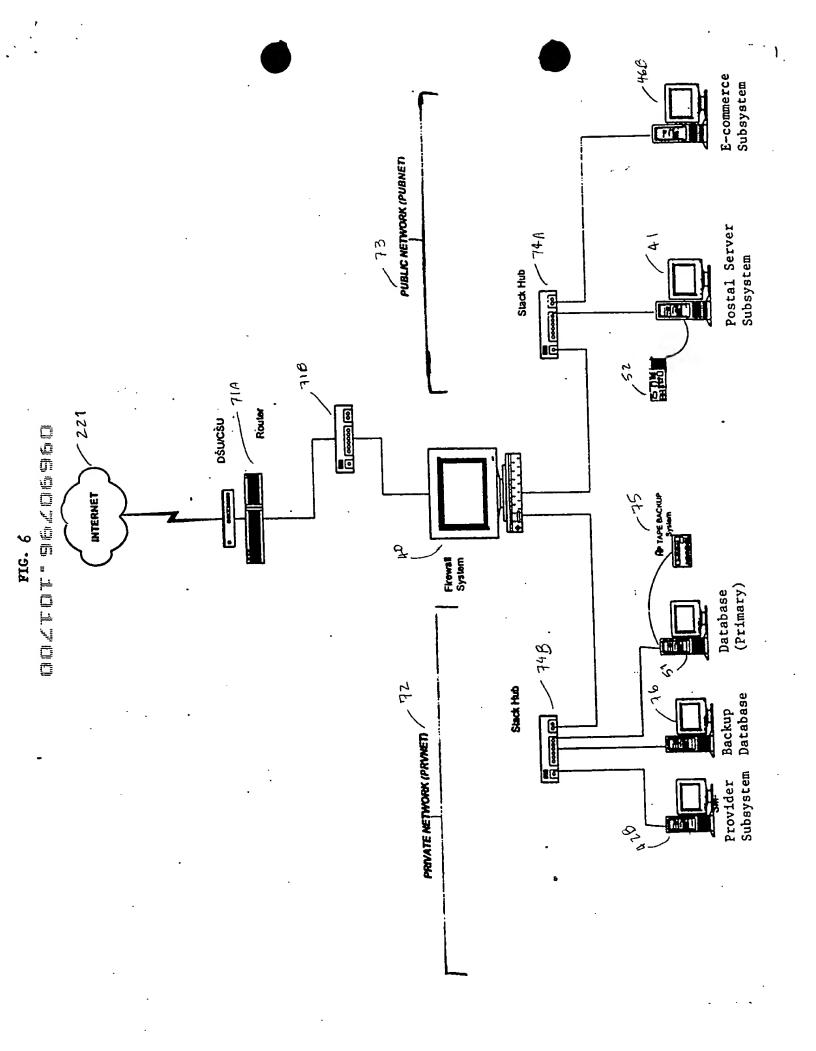
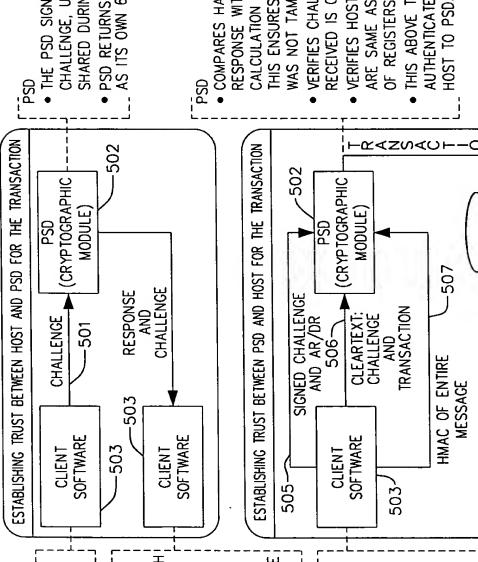


FIG. 7

GENERATES A RANDOM, 64-BIT CHALLENGE CLIENT SOFTWARE

THE CHALLENGE IT SENT WITH COMPARES THE HMAC OF THE HMAC IT RECEIVES CLIENT SOFTWARE FROM THE PSD.

- HOST TRUSTS THE PSD FOR THIS TRANSACTION.
- CHALLENGE TO AUTHENTICATE HOST RETAINS PSD'S ITSELF TO THE PSD
- CUSTOMER'S ASCENDING AND SIGNS CHALLENGE THAT THE PSD SENT, AND ALSO THE LOCAL RECORD OF THE DESCENDING REGISTERS. SENDS THIS TO PSD. CLIENT SOFTWARE
 - SENDS CLEARTEXT OF THE TRANSACTION MESSAGE. CHALLENGE AND THE
- SENDS AN HMAC OF ALL OF THE ABOVE, USING SHARED



 PSD RETURNS ABOVE, AS WELL AS ITS OWN 64-BIT CHALLENGE SHARED DURING REGISTRATION CHALLENGE, USING THE HMK • THE PSD SIGNS THE HOST'S

CALCULATION OF THE SAME. WAS NOT TAMPERED WITH. THIS ENSURES MESSAGE RESPONSE WITH LOCAL COMPARES HASH OF

- RECEIVED IS CHALLENGE SENT. VERIFIES HOST'S REGISTERS VERIFIES CHALLENGE
 - ARE SAME AS LOCAL DATA THIS ABOVE TWO STEPS AUTHENTICATE THE OF REGISTERS.

PSD PERFORMS TRANSACTION

DATABASE